Special Issue

New Advances in Cryptographic Theory and Application

Message from the Guest Editors

Post-quantum cryptography (PQC) is used to develop cryptographic algorithms that would be secure against both quantum and classical computers. These algorithms could serve as replacements for our current public-key cryptosystems to prepare for the eventuality that large-scale quantum computers become a reality that would completely break most existing public-key cryptosystems in use. Privacy-enhancing cryptography (PEC) refers to advanced cryptographic tools that can be used to achieve privacy goals in myriad applications. The technical challenge is often to enable parties to interact meaningfully toward achieving an application goal without revealing extraneous private information to one another or to third parties. Typical PEC techniques cover homomorphic encryption, secure multi-party computation, zero-knowledge proofs, and blind and ring signatures. With blockchain cryptography, we solicit new advances of research on, but not limited to, blockchain consensus protocols, multi/aggregate-signature, threshold cryptography, and succinct non-interactive arguments.

Guest Editors

Prof. Dr. Yunlei Zhao

Prof. Dr. Yu Yu

Dr. Shi Bai

Deadline for manuscript submissions

31 August 2025

Mathematics

an Open Access Journal by MDPI

Impact Factor 2.2
CiteScore 4.6

mdpi.com/si/156839

Mathematics
Editorial Office
MDPI, Grosspeteranlage 5
4052 Basel, Switzerland
Tel: +41 61 683 77 34
mathematics@mdpi.com

mdpi.com/journal/mathematics

Mathematics

an Open Access Journal by MDPI

Impact Factor 2.2
CiteScore 4.6

mdpi.com/journal/mathematics

About the Journal

Message from the Editor-in-Chief

The journal *Mathematics* publishes high-quality, refereed papers that treat both pure and applied mathematics. The journal highlights articles devoted to the mathematical treatment of questions arising in physics, chemistry, biology, statistics, finance, computer science, engineering and sociology, particularly those that stress analytical/algebraic aspects and novel problems and their solutions. One of the missions of the journal is to serve mathematicians and scientists through the prompt publication of significant advances in any branch of science and technology, and to provide a forum for the discussion of new scientific developments.

Editor-in-Chief

Prof. Dr. Francisco Chiclana
School of Computer Science and Informatics, De Montfort University,
The Gateway, Leicester LE1 9BH, UK

Author Benefits

High Visibility:

indexed within Scopus, SCIE (Web of Science), RePEc, and other databases.

Journal Rank:

JCR - Q1 (Mathematics) / CiteScore - Q1 (General Mathematics)

Rapid Publication:

manuscripts are peer-reviewed and a first decision is provided to authors approximately 18.4 days after submission; acceptance to publication is undertaken in 2.4 days (median values for papers published in this journal in the first half of 2025).